CHAINYARD

an IT People Company

Own And Control Your Identity: Identity Management Using Blockchain

Mohan Venkataraman – CTO, Chainyard
Jake Gostylo – Director, Content Innovation, D&B | October 2019

dun & bradstreet

Let's look at the world today…

Fraud in the US is a **$600B a year** drain on business.

https://www.bizjournals.com/nashville/stories/2007/10/15/focus4.html

Globally, fake goods is a **$500B a year** problem.

https://www.oecd.org/newsroom/trade-in-fake-goods-is-now-33-of-world-trade-and-rising.htm

The start to fighting all the business losses in fraud is advances in identity and identity management

By way of introduction

Jake Gostylo – Director of Data Innovation

Dun & Bradstreet: The global leader in commercial data offering insights on over 330M entities globally through the Dun & Bradstreet Data Cloud and solutions it powers.

Mohan Venkataraman – CTO of Chainyard

In partnership with IBM and over 10 major brands we are launching the Trust Your Supplier (TYS) network for supply chain onboarding.

AGENDA

- The TYS Network
- Self-Sovereign Identities
- Decentralized ID
- Why Blockchain

- What is an attestation
- Why Dun & Bradstreet is interested in the business of attestations
- How will business interactions improve

- What does this mean for IoT
- How does this scale for IoT applications

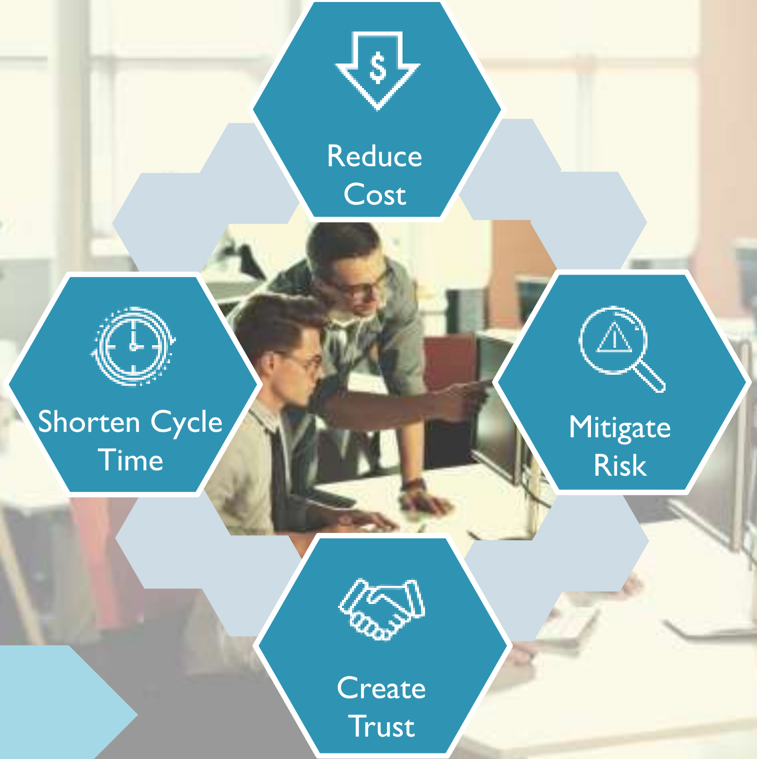
OBJECTIVE

Create a **Trusted Source of Supplier Information and Digital Identity**

that simplifies and accelerates

Supplier Onboarding and Lifecycle Management

A Single *SSI* based Supplier Digital Passport



What is Identity?

–Identity is a **set of characteristics that an entity (Person, Organization or Thing) identifies as belonging uniquely to them** embodying both changeable and unchangeable traits obtained naturally or provided by external bodies.

- Traditionally multiple identifiers issued by multiple bodies, centrally controlled, and can be restricted or revoked by the identity issuer at will

–**Self-sovereign identity**, can be defined as a lifetime portable digital identity that does not depend on any centralized authority.

- Its a new class of identifier that fulfills all four requirements: persistence, global resolvability, cryptographic verifiability, and decentralization

Why SSI?

–Enables a **person, corporation or a thing** to determine what constitutes their identity

–Securely share **portions or in-full** with one or more parties, claims made about their identity in a verifiable manner

–Carry **identity across geographic, business and economic boundaries**

–**Self manage** claims and reputation by identity holder

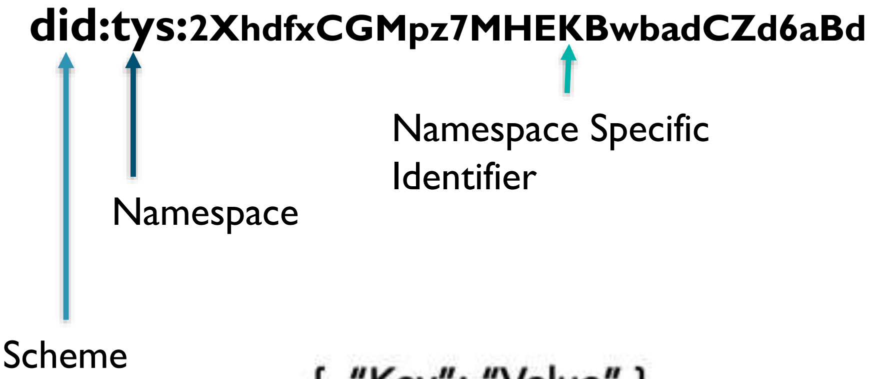
–Enables issuers of verifiable claims to **revoke or update the claims** as information surrounding them changes

Leverages Decentralized PKI, Decentralized Identity and the Blockchain

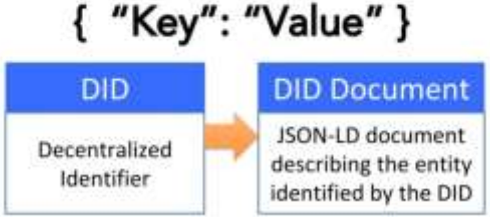
The TYS Decentralized Identifier (DID)

DID with Base58 or Base64 Encoding

did:tys:<left 20 bytes(sha256_hash(did_public_key)

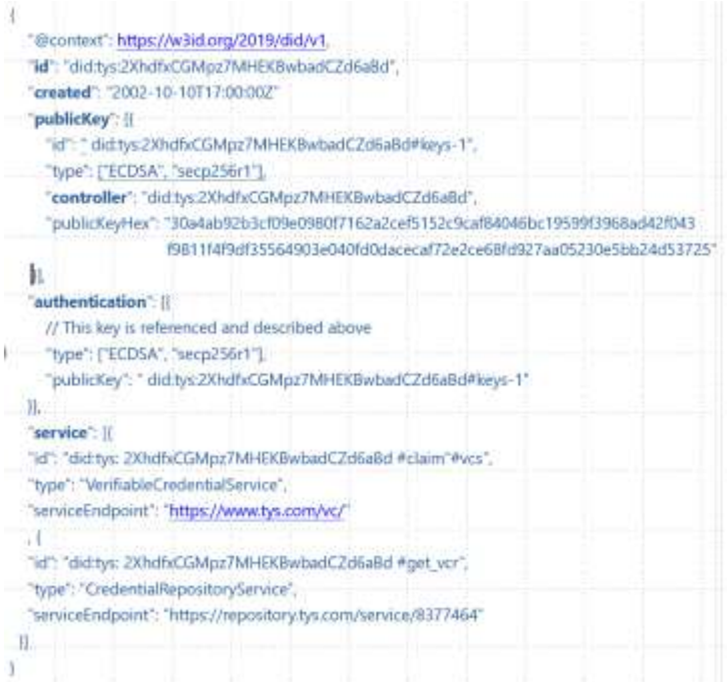


did:tys:2XhdfxCGMpz7MHEKBwbadCZd6aBd



{ "Key": "Value" }
DID
Decentralized Identifier
DID Document
JSON-LD document describing the entity identified by the DID

DID Document



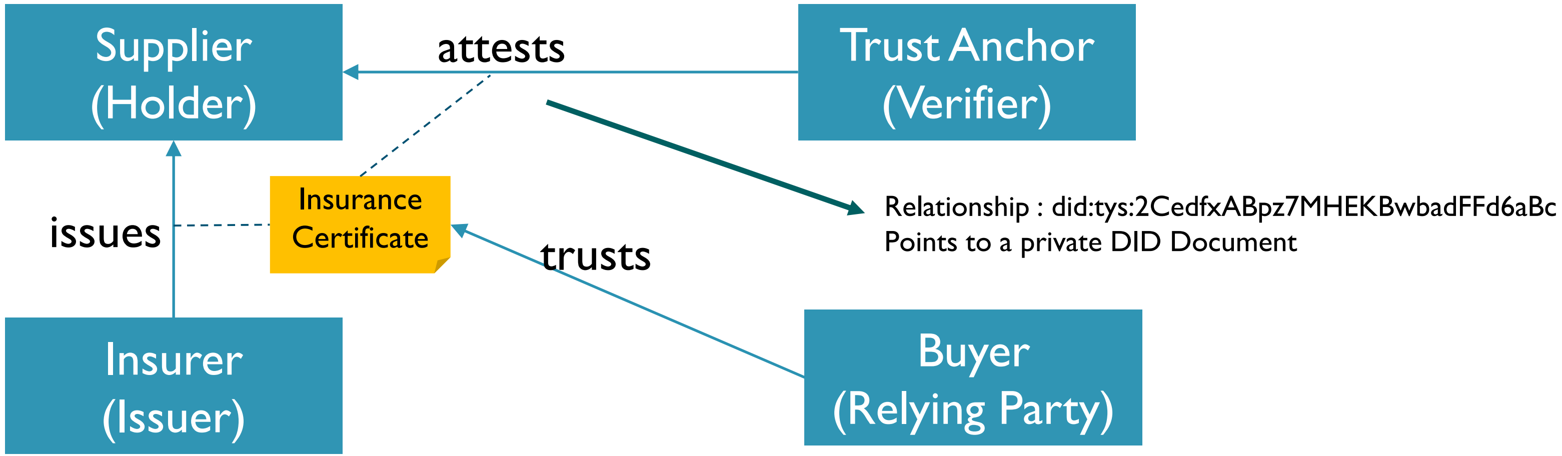
```
{
  "@context": https://w3id.org/2019/did/v1,
  "id": "did:tys:2XhdfxCGMpz7MHEKBwbadCZd6aBd",
  "created": "2002-10-10T17:00:00Z"
  "publicKey": [{
    "id": " did:tys:2XhdfxCGMpz7MHEKBwbadCZd6aBd#keys-1",
    "type": ["ECDSA", "secp256r1"],
    "controller": "did:tys:2XhdfxCGMpz7MHEKBwbadCZd6aBd",
    "publicKeyHex": "30a4ab92b3cf09e0980f7162a2cef5152c9caf84046bc19599f3968ad42f043
                    f9811f4f9df35564903e040fd0dacecaf72e2ce68fd927aa05230e5bb24d53725"
  }],
  "authentication": [{
    // This key is referenced and described above
    "type": ["ECDSA", "secp256r1"],
    "publicKey": " did:tys:2XhdfxCGMpz7MHEKBwbadCZd6aBd#keys-1"
  }],
  "service": [{
  "id": "did:tys: 2XhdfxCGMpz7MHEKBwbadCZd6aBd #claim"#vcs",
  "type": "VerifiableCredentialService",
  "serviceEndpoint": "https://www.tys.com/vc/"
  , {
  "id": "did:tys: 2XhdfxCGMpz7MHEKBwbadCZd6aBd #get_vcr",
  "type": "CredentialRepositoryService",
  "serviceEndpoint": "https://repository.tys.com/service/8377464"
 }],
}
```

Globally Unique Identifier that resolves to DID Document

Digital Identities in TYS

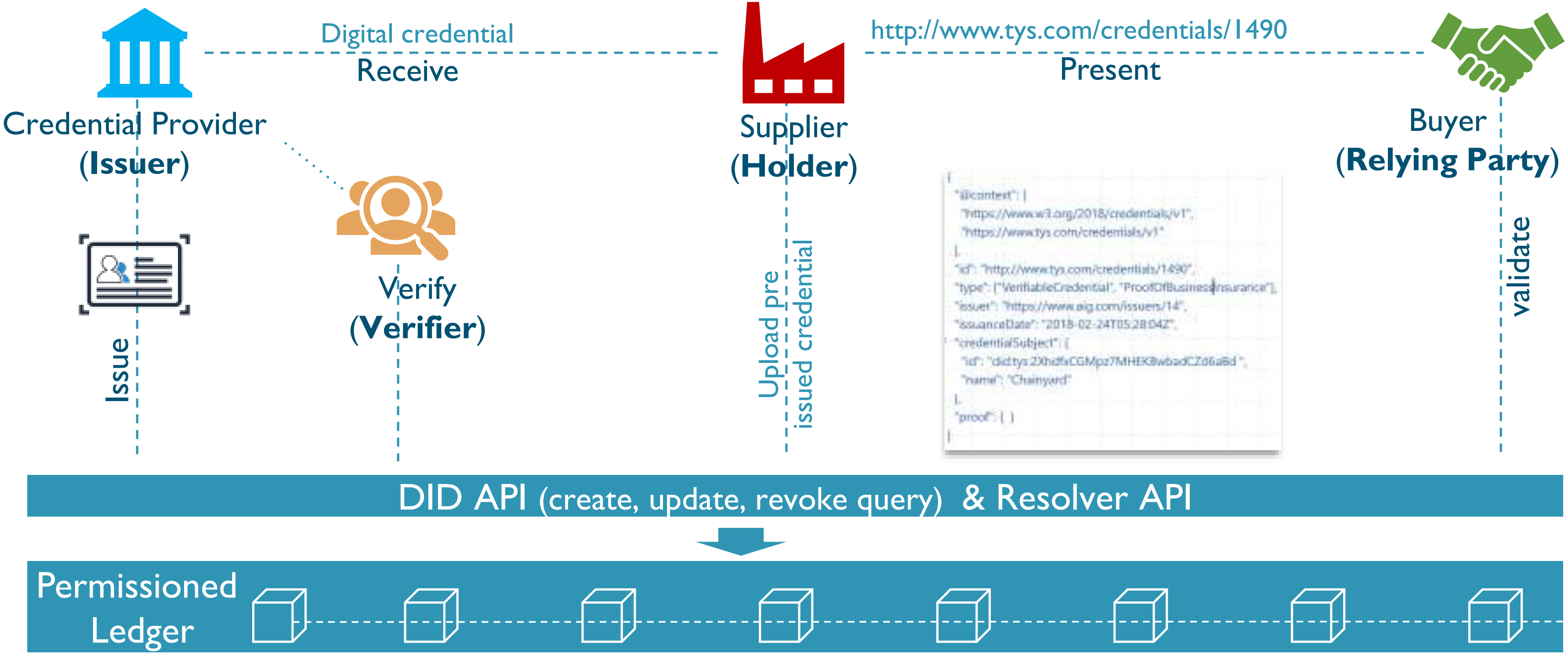
- DID : Digital Identity representing an Individual, Organization or Thing
- Pairwise DID : Digital Identity associated with a Relationship, and resolves to a private DDOC document; (can be public) stored on sideDB or a private channel

Supplier DID: did:tys:2XhdfxCGMpz7MHEKBwbadCZd6aBd



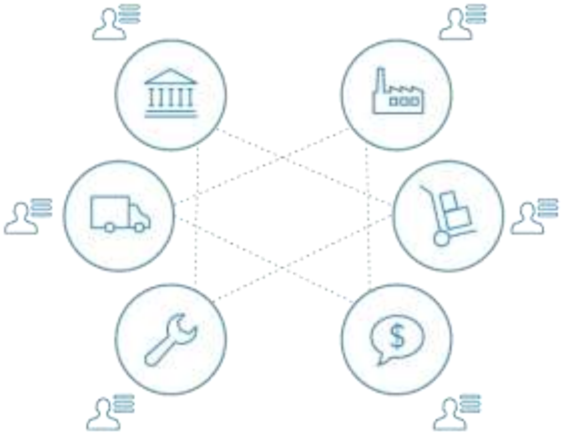
Relationship : did:tys:2CedfxABpz7MHEKBwbadFFd6aBc
Points to a private DID Document

DIDs and Blockchain (TYS)



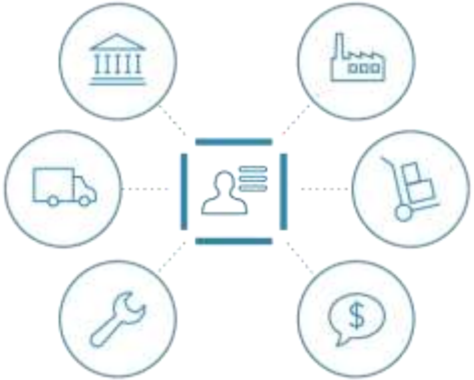
```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://www.tys.com/credentials/v1"
 ],
 "id": "http://www.tys.com/credentials/1490",
 "type": ["VerifiableCredential", "ProofOfBusinessInsurance"],
 "issuer": "https://www.aig.com/issuers/14",
 "issuanceDate": "2018-02-24T05:28:04Z",
 "credentialSubject": {
  "id": "did:tys:2XhdfxCGMpz7MHEK8wbadCZd6aBd",
  "name": "Chainyard"
 },
 "proof": { }
}
```

Trust Your Supplier – Why Blockchain



Conventional Systems are open to error, fraud and inefficiency

- In conventional systems each participant has his own, separate database, or ledger — increasing the possibility of human error or fraud
- Shared databases cannot prevent malicious activity. Hacked entities can corrupt or destroy data in the shared database, making it invalid for everyone involved.
- Reliance on intermediaries for validation creates inefficiencies
- Often laden with manual processes, resulting in frequent delays and inefficiencies



Blockchain is designed for trust and secure trading

- Single, shared, tamper-evident ledger — once recorded, transactions cannot be altered
- Provides levels of error checking and transaction validity not obtainable in regular shared databases.
- Data is guaranteed to be valid and reconciled against the data held by the others participating on the Blockchain.
- Immutably records all details of a transaction end-to-end, reducing vulnerabilities.

Blockchain Provides a Trusted, Common, Single Version of the Truth

Historical Milestones for attestations

RSA

1977 – The first algorithms published that provide provable digital signature produced from a private key.

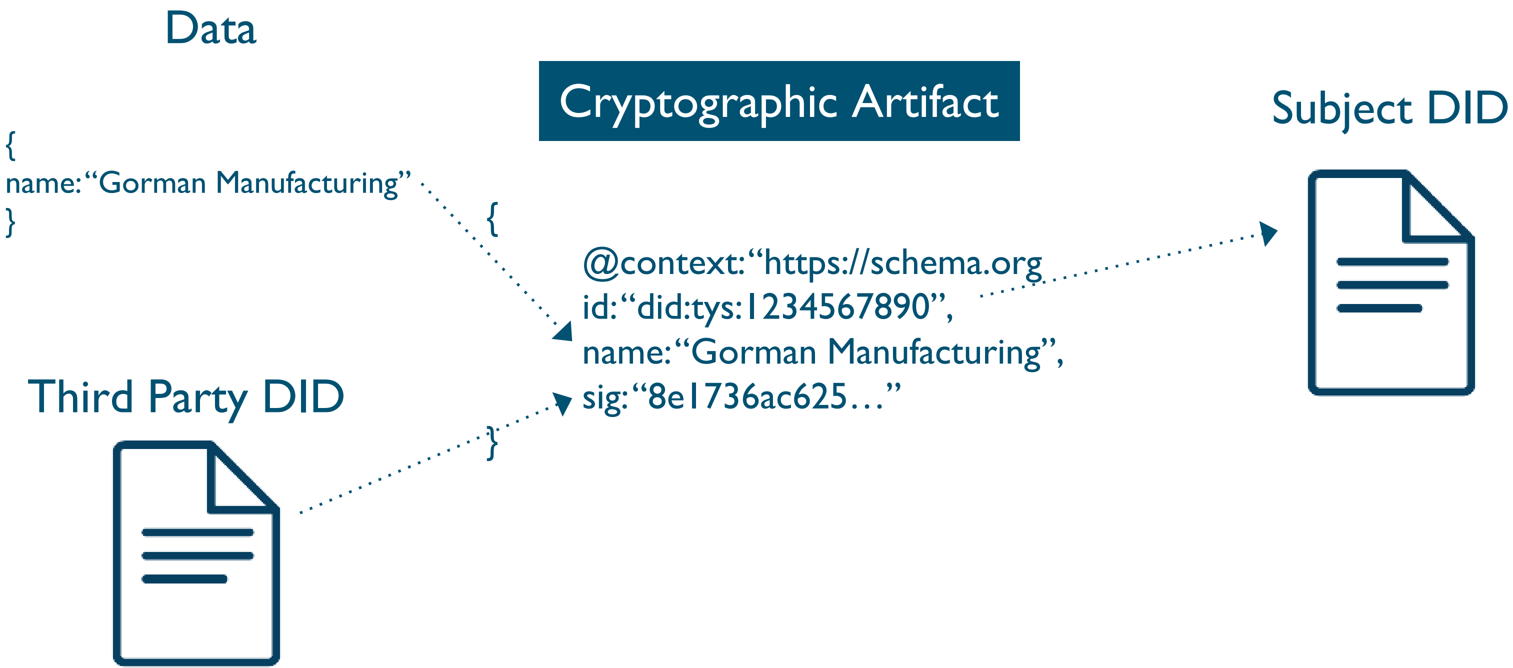
x.509

1988 – Commercially viable attestations of one cryptographic artifact to another. Strict authority hierarchy.

WoT

1992 – Web of Trust introduced with PGP as a distributed way to manage attestations. Graph techniques used to judge validity.

What is an attestation?



Data

```
{
name:“Gorman Manufacturing”
}
```

Cryptographic Artifact

```
{
@context:“https://schema.org
id:“did:tys:1234567890”,
name:“Gorman Manufacturing”,
sig:“8e1736ac625…”
}
```

Subject DID

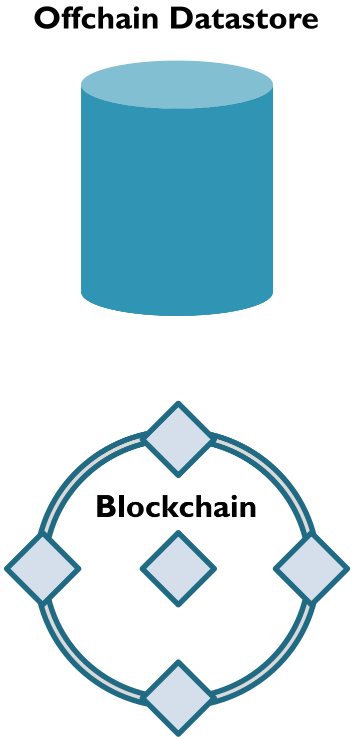
Third Party DID

Where do attestations belong?

Attestations should not be pushed to a blockchain, not even encrypted.

Encrypt(data)

Hash(data + nonce)



Why does Dun & Bradstreet care about this?

CHANGING THE PARADIGM

- Much more transparency in the process. No longer is the buyer is getting data that the seller knows nothing about.

- Follows the strictest intent of General Data Protection Regulation (GDPR).

- Closer interaction with the entity we have data on will allow positive feedback loop for increased data quality.

How will businesses benefit?

RFP process can have the vetting frontloaded. No more going back to the drawing board.

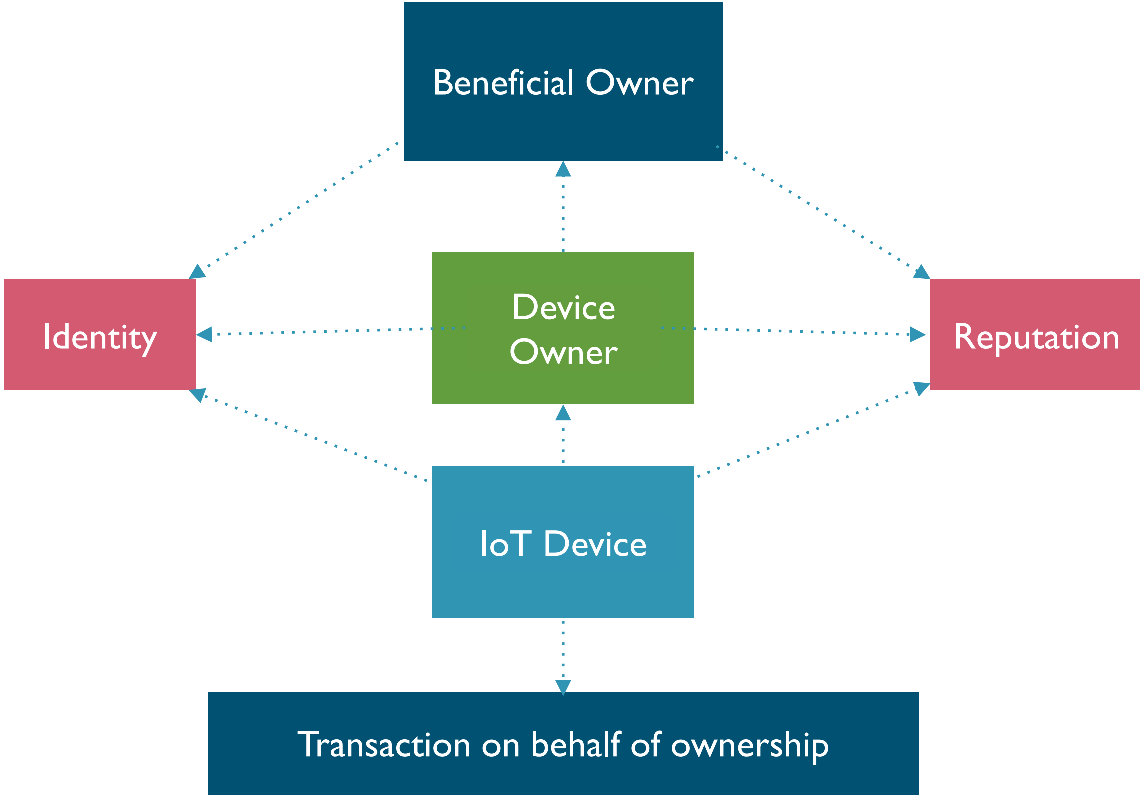
Suppliers don't have to fill out different questionnaires for every engagement.

Suppliers have greater transparency in how they are presented.

The number of necessary touch points with third party data decreases.

The bottom line is that all parties get reliable data faster.

What does Identity look like in an IoT business context



Beneficial Owner

Identity

Device Owner

Reputation

IoT Device

Transaction on behalf of ownership

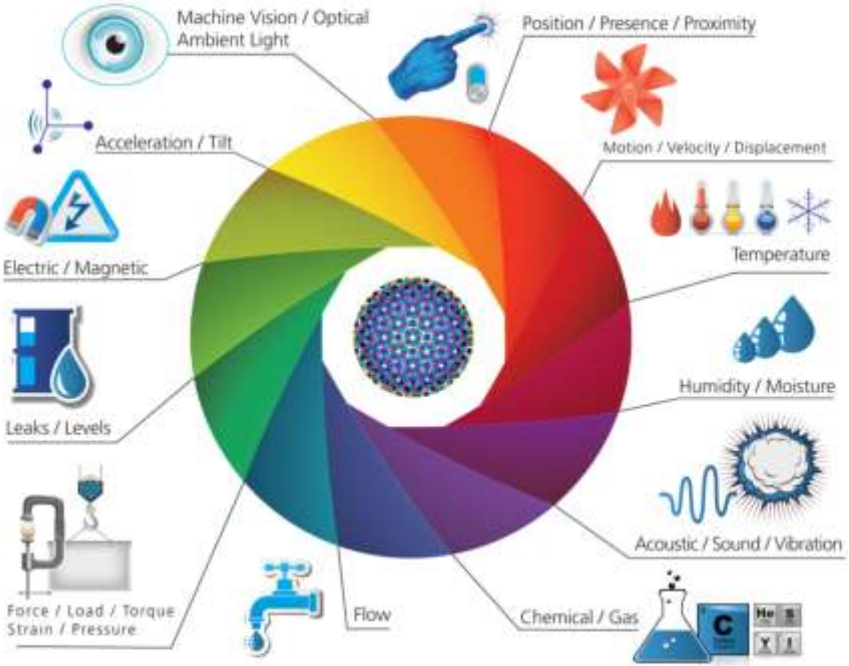
IoT, Identity and Blockchains

- IoTs play a critical role in enabling efficient, fraud and counterfeit proof, auditable supply chains
- Authenticating and authorization of IoT devices through digital identities is a critical aspect of preventing intrusion and hacking of business processes
- IoT devices provide verifiable credentials and attest supply chain transactions
- IoT Devices can be applied for various purposes such as location capture, imaging, motion detection, altitude, tilt, light exposure, route deviations, acceleration
- Smart Tags such as RFID, NFC Chips, Chemical and Optical Tags provide verifiable credentials to products
- DIDs provide credentials to parties and/or assets in the supply chain such as product, suppliers, transporters and logistics operators
- Combined with Digital Identities and Smart Tagging Technologies, IoT and Blockchain provide higher levels of trust in ensuring **supplier credibility** and **product authenticity**

IOT Landscape

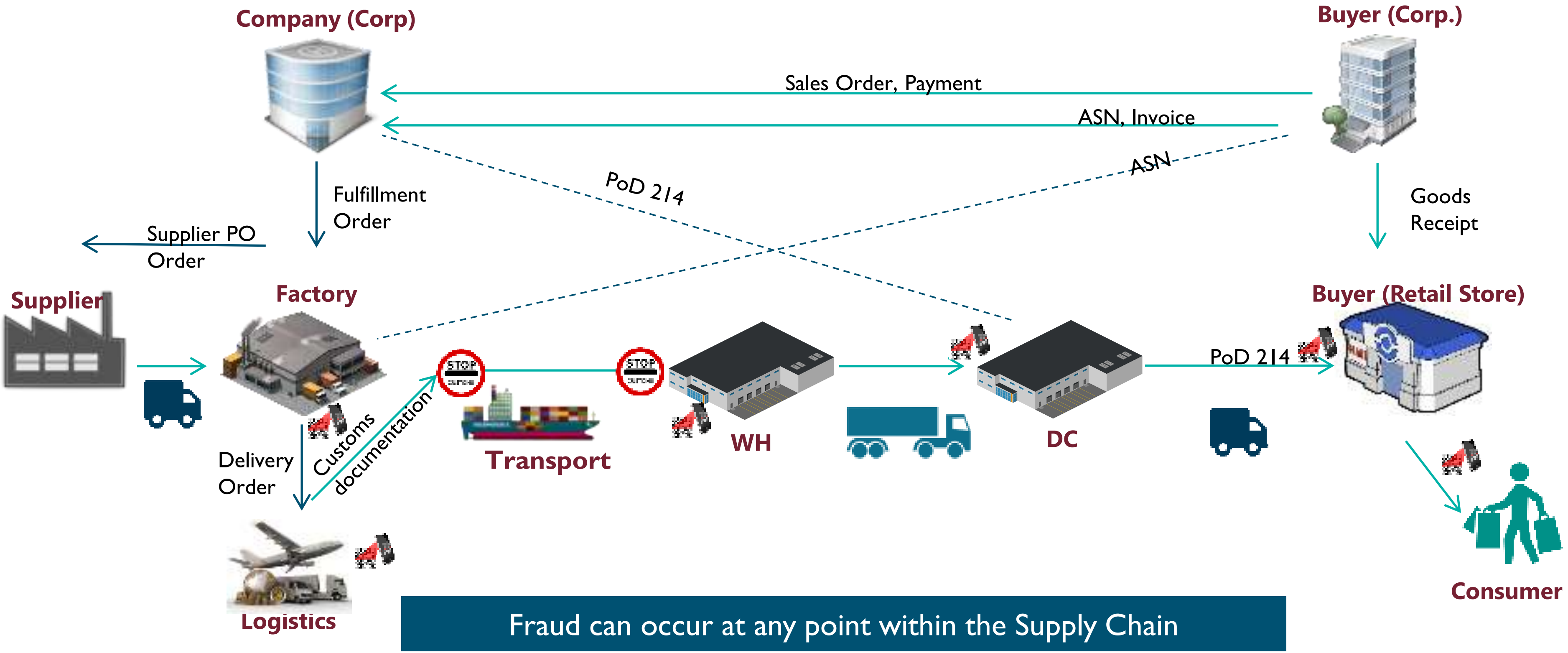
1 SENSORS & ACTUATORS

We are giving our world a digital nervous system. Location data using GPS sensors. Eyes and ears using cameras and microphones, along with sensory organs that can measure everything from temperature to pressure changes.



Source: Postscapes and Harbor Research

Supply Chain – From Seller to Buyer



Fraud can occur at any point within the Supply Chain

This Photo(s) by Unknown Author is licensed under CC BY

The Future of Verifiable Credentials

IoT and Blockchain In Supply Chain

Blockchain Assigns DID

Manufacturer
Assigns Smart Tag
Maps to Product Code/Serial#

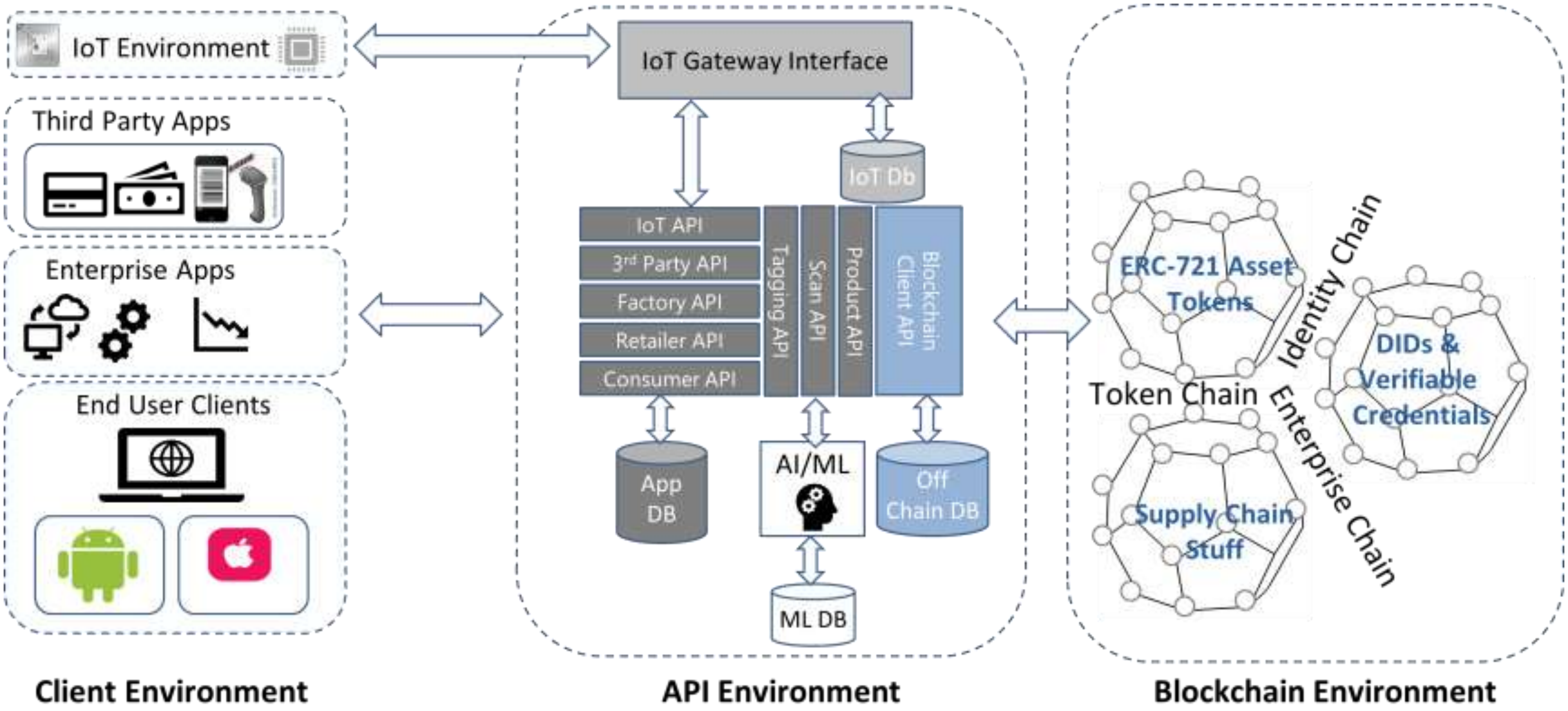
IoT Devices
Records Proof of Supply Chain Process

Retailer
Issues Proof of Cryptographically Verifiable Proof-of-Purchase Cert.

F682BC0EF6CF00D777C2EA7AEFDD9B548A892
91728FD2C349D6A5E83BD77A85B

Tokenization
Assigns Cryptographic ERC-20 Proof of Ownership Token

A Conceptual Architecture



Thank You

CHAINYARD
an IT People Company

dun & bradstreet